Outline

- Background
- XP/IE6/Office 2003 Implementation
- Vista/IE7/Office 2007 Implementation
- Benefits
- Key Actions
- Vista Conclusion

FDCC

USAF Then and Now

Status in Nov 2005

- 100's of PC Software Baselines
- Programs/bases built configurations
- Average user could install software
- No AF level configuration manager
- 100+ days to install security patches
- Slow adoption of new technology
- Variety of systems management tools
- No software development policy
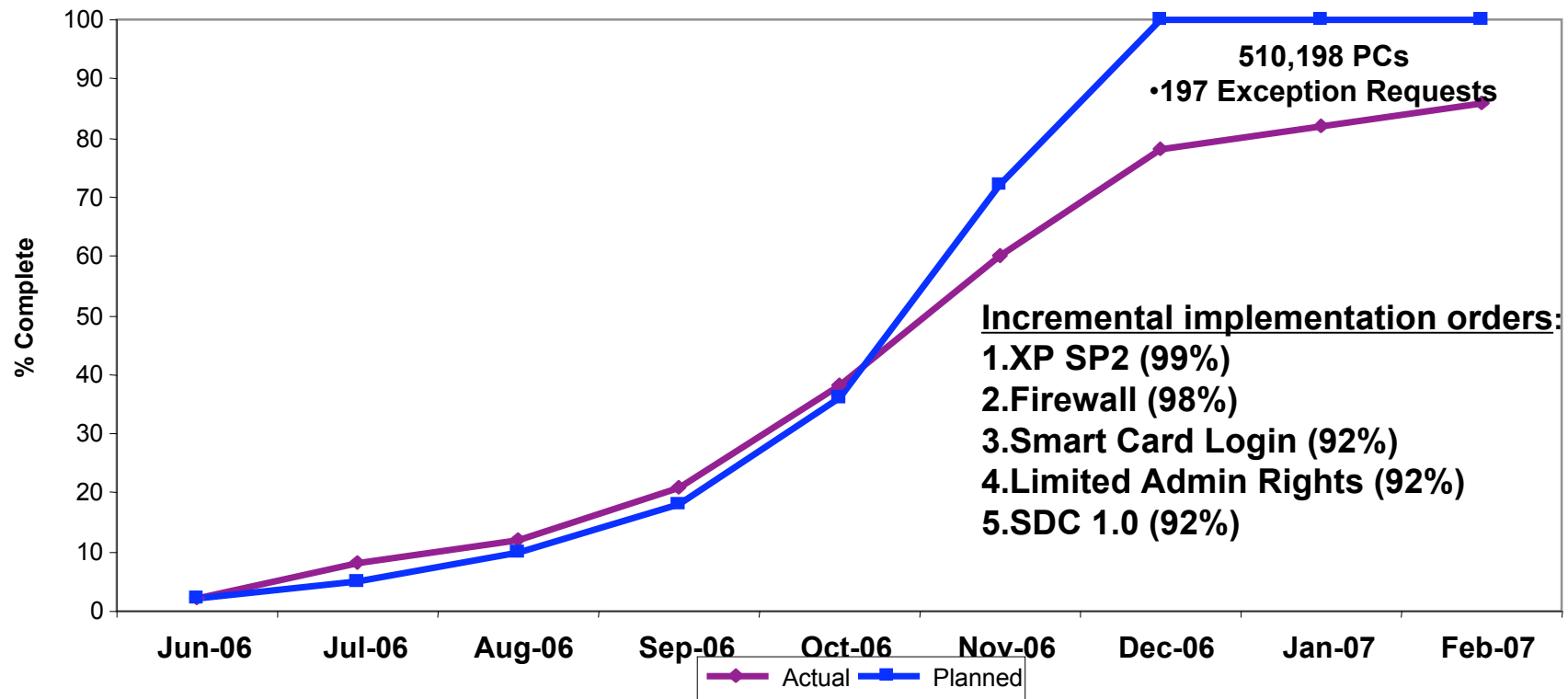- Periodic vulnerability reporting

2006-2008 Desired Outcomes

- ☑ AF Standard Configurations
- ☑ AF Level Configuration Mgt
- ☑ Limit system admin privileges
- ☑ AF level configuration manager
- ☑ Rapid Patch Mgt Process
- ☑ Plan for early adoption decision
- ☑ AF standard toolset with procedures
- ☑ AF Development/Test policy
- ☐ Automated Comply and Connect

FDCC

SDC 1.x AF Wide Deployment Metrics (XP/Office 2003/IE6)
Goal: 100% by 31 Dec 06

Standard Desktop Configuration

510,198 PCs
•**197 Exception Requests**

Incremental implementation orders:
1. **XP SP2 (99%)**
2. **Firewall (98%)**
3. **Smart Card Login (92%)**
4. **Limited Admin Rights (92%)**
5. **SDC 1.0 (92%)**

% Complete (y-axis: 0, 10, 20, 30, 40, 50, 60, 70, 80, 90, 100)

x-axis: Jun-06, Jul-06, Aug-06, Sep-06, Oct-06, Nov-06, Dec-06, Jan-07, Feb-07

Legend: Actual — Planned

As of 10 Apr 2007

The Air Force SDC 1.x is almost identical to the XP FDCC

FDCC

Deployment Options Used for XP and Vista

- Manual Wipe and Load from a DVD
- Operating System Deployment (OSD). User data is migrated automatically and some applications will be reinstalled
- Upgrade in Place from XP over the network using SMS
- Pre-installed on new PC's (8,500 with Vista as part of test)

FDCC

Toughest Challenges

- Removing local admin rights from normal users
  - Restricts installing software from CD or Internet
  - Restricts disabling of security settings
  - Restricts deviations from the enterprise standard
  - Restricts a worm/virus from inheriting admin access
- Testing applications to function without a user having local admin rights
  - Why? Who Pays? How? This too shall pass?
- A "simple, easy and trustworthy" deployment process using automated network tools

FDCC

Governance

- General Officer Steering Group
- Standard Settings Review
- CIO Policy
- Network Command and Control Authority
- Enterprise Configuration Control Board
- Program Office, Plan, Schedule
- Exception/ Waiver Process
- Metrics and reporting

Foundation for Digital Comply and Connect Governance

FDCC

SDC 2.0 Benefits
(Vista, Office 2007, IE 7)

Security

- User Account Control to limit privileged system access
- IE 7 runs in "protected mode" on Vista
- Windows Services Hardening and Memory Randomization
- Firewall (inbound and outbound) that can be controlled by group policy
- Data encryption capabilities
- "Comply and Connect" Network Access Protection Client

Manageability

- 600+ new network group policy settings many of which are not set in FDCC
- Power management controls

Other Improvements

- More powerful search in Vista and Office 2007
- User Interface -- ease of use
- Single product for 32-bit and 64-bit computers; easier migration to 64 bit
- Native IPv6 foundation that can be consistently installed AF and DoD wide
- New file formats; less storage required
- Improved deployment capabilities for SDC disk image (WIM, BDD)

FDCC

DoD SDC Standard Settings Reviews (For the Image and Group Policies)

	Total Available Settings	Microsoft Security Guide Settings	NSA/DISA Security Guide Settings	Air Force Baseline Settings (Nov 9)	Navy Baseline Settings (Dec 8)	Army Baseline Settings (Feb 7)	DoD SDC (9 Apr 2007)
Vista (Security Only)	217	217	0	279	251	293	217
Vista (other GPO settings)	1258	36	14	244	268	244	244
Office 2007	173	NA	-	173	173	173	173
Internet Explorer 7	1192	99	32	162	162	162	162
Major Delta's from NSA/DISA	-	46	-	7	9	6	NA

•Notes:
1. Organizations participating included NIST, NSA, DISA, DHS, Microsoft, Army, Navy, Air Force, Marines
2. Experts in information assurance, system administration, network operations/defense, cryptology, help desk, and system engineering.
3. Established other types of settings beyond security (e.g., performance, usability, compatibility, and features)
4. DoD SDC settings will be reviewed again after each military service completes operational testing
5. Each military service is evaluating variations of some settings to obtain feedback for DoD

Over 5,000 man-hours in Joint Meetings to arrive at consensus

FDCC

USAF SDC 2.0 (Vista/Office 2007/IE 7) Plan

☑ Nov 06 - Establish USAF baseline configuration settings/features

☑ Jan 07 - Develop detailed plan and schedule

☑ Jan 07 - Build initial USAF test configuration

☑ Feb 07 - Test/Validate baseline configuration

☑ Feb 07 - Test Hardware Compatibility and Performance

☑ Mar 07 - Test software applications for compatibility

☑ Mar 07 - Test XP with IE7at 8 lead bases (SDC 1.3)

☑ Apr 07 - Establish DoD Standard Desktop Configuration

☑ Jun 07 - Test XP with Office 2007 at 8 lead bases for (SDC 1.5)

☑ Jul 07 - Test Vista, Office 2007, IE 7 at 8 lead bases (SDC 2.0)

☺ Oct 07 - Earliest timeframe for approved USAF use

☺ Jan 09 - Earliest timeframe for mandatory USAF Vista use

U.S. Army, Navy, and Marines have a similar plan being executed in parallel

OMB FDCC Configuration Leverages much of the DoD Work

FDCC

Benefits of a Federal Core Configuration

- A proven "best practices" configuration
- Federal policy and regulation support
- NIST provided automated compliance audit tools
- Support from OMB, NIST, Microsoft, DHS, industry 3rd parties, other Agencies (e.g., NSA, DoD)
- Target platform for developed or purchased software
- Federal wide problems solved once for all
    - License activation, settings, power mgt., cryptology, IPv6, features, cyber security, performance, PKI certificates, testing, platform and application certification, automated verification
- Deploy patches faster and more successfully
- Reduce operating system, user and applications vulnerabilities
- Reduce support calls for IT help desks

One U.S. Federal Govt, One Core Configuration Management Process

This slide represents the views of the presenter and not the Federal Government

FDCC

Key Actions

- Remove local admin rights for normal users ASAP
- Decide on XP SP2, Vista or Both
- Decide if Vista/IE7 will be installed on new PCs
- Build/Test configuration(s) based on FDCC
    - Start applications compatibility testing ASAP
        - Use automated tools to identify likely incompatibilities (ACT 5)
        - Fix, virtualize or remove those that are incompatible
    - Ensure <u>new</u> hardware will support Vista
    - Select deployment approach, process and tools
    - Analyze current hardware and software
- Select representative lead pilot installs
- Enterprise Governance, Configuration management, and Metrics

Assess, Plan, Build, Test, Deploy, Improve

FDCC

Key Actions

- Have a good communications plan for end users and administrators (Newsletters, emails to Help Desk)
- Expect that users will accept the change if they understand the need for change
- Establish a feedback mechanism to get end user feedback and advise them
- Use free training on Office 2007 & Vista on Microsoft's web site
- Use the tools that Microsoft and other vendors provide (e.g., BDD, ACT 5, WVBA, and SMS)

FDCC

SDC 2.0 Conclusions Thus Far

- Internet Explorer 7 has been approved for use; some incompatible applications
- Office 2007 can be installed with only minor "first 24 hour" impacts on users
- Vista is accepted by end users in 3 days
- Major challenge: Simple, Easy, and Trustworthy remote unassisted installs and upgrades

FDCC

Conclusion

- A "Window" of opportunity to implement enterprise configuration management the first time for Vista
- Requires Agency leadership buy-in
- Requires program and change management
- Makes security less expensive and more effective for everyone
- One time challenges of admin rights and applications compatibility
- Jump start materials provided today

FDCC